Innominate mGuard

Version 7.2.1 - Release Notes

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin, Germany
Tel.: +49 30 921028-0
e-mail: contact@innominate.com
http://www.innominate.com/

Copyright © 2003-2010 Innominate Security Technologies AG

December 2010
“Innominate” and “mGuard” are registered trademarks of the Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.
mGuard technology is protected by the German patents #10138865 and #10305413. Further national and international patent applications are pending.
No part of this documentation may be reproduced or transmitted in any form, by any means without prior written permission of the publisher.
All information contained in this documentation is subject to change without previous notice. Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes. In addition, Innominate is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.
This documentation may not be photocopied, duplicated or translated into another language, either in part or in whole, without the previous written permission of Innominate Security Technologies AG.

Innominate Document Number: RN207212C10-031

Vertical bars to the left mark significant changes in comparison to the release notes for firmware version 7.2.0.

1 Product Description

1.1 Supported Hardware

The firmware can be operated on the following hardware platforms:

- mGuard centerport
- mGuard industrial RS
- mGuard smart²
- mGuard smart
- mGuard core
- mGuard PCI
- mGuard blade
- EAGLE mGuard / mGuard industrial
- mGuard delta

For detailed information about these platforms please see the technical data sheets, which are offered for download at http://www.innominate.com/ .

1.2 Software Features

The firmware provides the functionality of a network firewall with support for VPN connections (license controlled) and other services. The complete features are listed and described in detail within the user manual, which can be downloaded from http://www.innominate.com/ .

1.3 Changes Since Previous Release

This section lists the changes since the previous release. Changes since earlier versions are listed in the chapter “Version History” below.

1.3.1 Changes made between 7.2.0 and 7.2.1

- Version 7.2.1 adds support for a new hardware revision of the EAGLE mGuard product

1.4 Updating from previous releases

No update is provided for the 7.2.1 release, since the changes solely concern a new hardware revision of the EAGLE mGuard product. Devices running firmware version 7.2.0 don't need to be upgraded.

1.4.1 Important installation information (flashing with 7.2.1)

- Devices which have been shipped with firmware version 2.x.y or earlier need to be flashed or updated to firmware 4.1.x or 4.2.x first to get the boot loader updated.
- Devices produced before 2007 require **two** Major Upgrade Licenses before the 7.2.1 firmware image can be installed using the flash mechanism.
- If such a device had already been updated or flashed to any 5.x.y version successfully beforehand then just **one** Major Upgrade License is required for it.
- Devices produced before October 2007 require **one** Major Upgrade License before the 7.2.1 firmware image can be installed using the flash mechanism.
- Younger devices do not need a Major Upgrade License.
- If the device is flashed with 7.2.1 without appropriate license its error LED will signal the morse code “SOS” whenever it is started.
- The Major Upgrade License must be obtained for each device while it still

operates firmware version 4.1.x, 4.2.x, or 5.x.y. Flash it with firmware 4.1.x, 4.2.x, or 5.x.y first if necessary. Please see their respective release notes and manual for details.

- To obtain a Major Upgrade License, a Major Upgrade Voucher needs to be purchased and redeemed first. The voucher must be cached with the help of the "Edit License Request Form" feature available within the "Management / Licensing" menu of the device. The device must therefore be connected to the Internet, for example by operating it in auto stealth mode and attaching it to a PC which is connected.
- The Major Upgrade License must be stored as a file.
- The license file must be copied to the tftp directory as a file named "licence.lic" in the same directory as the firmware image (file "jffs2.img.p7s").
- If two licenses are needed for a device, then only the one downloaded at last must to be copied to the tftp directory.
- Once a device has been flashed with firmware 6.x.y or 7.x.y successfully, further flashing of that device with firmware version 7.2.1 or older will not require any license file to be present within the tftp directory.
- The installation of the 7.2.1 firmware image (file "jffs2.img.p7s") must be performed with exactly the file "install.p7s" it was shipped with. For the mGuard centerport the file names are "firmware.img.x86.p7s" and "install.x86.p7s" respectively. For the mGuard smart² the file names are "ubifs.img.mpc83xx.p7s" and "install-ubi.mpc83xx.p7s" respectively.
- If a device needs to be downgraded from 7.2.1 to any older firmware version prior to 5.0.0, the file "install.p7s" from 7.2.1 must be used in combination with the older version's file "jffs2.img.p7s".

1.4.2 Obtaining the update files

As of release 3.0.0 customers must register before downloading the update files for offline download or to access the online update server. Please refer to

http://www.innominate.com/register_software
http://www.innominate.de/register_software.

After registration user and password information is sent. Please note that the update server is operating using the "https" protocol.

2 Version History

This chapter lists the changes between former versions of the mGuard firmware.

2.1 Changes made between 7.1.1 and 7.2.0

- Version 7.2.0 adds support for a new platform, the mGuard smart²
- Version 7.2.0 allows to assign a management IP address via BOOTP before it is accessed for configuration the first time, see section 5.2 of the manual
- Version 7.2.0 introduces a new style of the WebUI
- Version 7.2.0 fixes security issue CVE-2010-2240
- Version 7.2.0 fixes VPN license issues
- Version 7.2.0 fixes IPsec status display with regards to certificate subjects containing special characters
- Version 7.2.0 improves log messages for VPN connections which wait for a network interface to become ready

Version 7.2.0 improves the robustness of the WebUI on multiple logins authenticated through X.509 certificates

2.2 Changes made between 7.1.0 and 7.1.1

- Version 7.1.1 improves robustness of the upgrade process for devices with complex configuration or many saved configuration profiles.

2.3 Changes made between 7.0.2 and 7.1.0

- The NAT functionality is extended to allow masquerading of external IP addresses also.
- VPN connections with the setting “%any” for the peer address can now be bound to a particular network interface other than the external.
- Listening for TCP encapsulated VPN connections can be bound to another network interface than the external the same way.
- Listening for TCP encapsulated VPN connections is now supported even if the mGuard is located behind a port forwarding NAT gateway.
- Support for “Ring/Network Coupling” and “IPsec/L2TP” is re-activated.
- Support for automatic backup of each configuration change to the external configuration storage is added.
- Optional time-outs for stale SSH connections and SEC-Stick connections are added.
- Broken TCP packets (with all TCP flags cleared) can now optionally be forwarded within established TCP connections to work around defective network stacks of a few PLCs.
- Version 7.1.0 improves the robustness of its CIFS Integrity Checking feature.
- Version 7.1.0 fixes the behavior of the CMD contact in combination with archival of diagnostic messages for VPN connections.
- Version 7.1.0 fixes the behavior of the CMD contact in combination with an already enabled VPN connection.
- Version 7.1.0 fixes the CIFS AV Scan Connector with regards to proxying access to large volumes.
- Version 7.1.0 suppresses irritating port forwarding behaviour in combination with routing of the IP the port is forwarded to.
- Version 7.1.0 fixes the establishment of TCP encapsulated VPN connections in combination with a dynamic hostname as the peer address.
- Version 7.1.0 fixes the command “synup” for the CGI interface allowing to

control VPN connections.

2.4 Changes made between 7.0.1 and 7.0.2

- Fixed Linux kernel NULL pointer dereference: CVE-2009-3547
- Disabled openssl TLS renegotiation: CVE-2009-3555
- Fixed support for multiple TCP-encapsulated VPN connections
- Changed update procedure to refuse update from 6.1.x if AVP is enabled
- Fixed SEC-Stick login for user names containing a dash
- Fixed rarely seen TFTP timeout while flashing firmware
- Fixed remote access through VPN connection that are TCP-encapsulated

2.5 Changes made between 7.0.0 and 7.0.1

- Closed security issue CVE-2009-2692 for the Linux kernel
- Closed security issue CVE-2009-2185 for the VPN subsystem (Openswan)
- Closed security issue regarding an SSL attack for the "curl" software package which is relevant for the Configuration Pull mechanism only
- Fixed use of CRLs for acceptance of VPN connections
- Fixed restoring the factory default profile through the GUI
- Fixed restoring of former configuration profiles uploaded via GUI
- Fixed acceptance of the firmware update by all updateable devices
- Fixed license handling for VPN connections to allow an arbitrary number of configured VPN connections
- Fixed functionality of the DHCP server regarding dynamic IP address pools with just one IP address
- Fixed issue “netadmin cannot delete particular rows from a nested table”
- Fixed issue “VPN remote 1:1 NAT incomplete when tunnel enabled via CMD/CGI”
- Fixed access to the CIFS AV Scan Connector in Stealth modes
- Improved acceptance of configuration profiles which are transferred from one hardware platform to another

3 Identified Issues and Workarounds

Issue “No Access To 1.1.1.1 With Management IP Address Set”

	Description
Synopsis	If a management IP address is set in stealth mode(s), access via 1.1.1.1 fails.
Symptom	Access via 1.1.1.1 is not supported in static stealth or multiple client stealth mode, if a management IP address is configured.
Workaround / action	Use the management IP address also from the internal interface (protected port) to access the mGuard.

Issue “Power OK shown late on mGuard Blade”

	Description
Synopsis	The circuit checking the states of the redundant power supply units in the mGuard Blade does include filter capacitances. Due to these capacitances state changes are not signaled immediately. Power failure is signaled with a delay of 3-4 seconds, replacement of a power supply (now OK) is only signaled with a delay of 90 seconds.
Symptom	Display of the state of the power supply may still show failure even after the power supply has been re-enabled for 90s.
Workaround / action	None.

Issue “ICMP failure with transport VPN in Stealth Mode with SNMP”

	Description
Synopsis	ICMP echo requests are not answered through a transport mode VPN connection if the device is in Stealth Mode and SNMP is activated
Symptom	From a remote peer a client protected by an mGuard shall be pinged through a transport mode VPN. The tunnel is up and other traffic succeeds but ICMP echo requests are not answered. This problem only occurs if SNMP is enabled on the mGuard.
Workaround / action	None.

Issue “VPN firewall rule application for wrong tunnel”

	Description
Synopsis	If multiple tunnels are established to the same remote network originating from different local networks these tunnels conflict with one another.
Symptom	Firewall rules intended to be used within one tunnel are applied to connections of another one. Only one of those tunnels with the same remote network can be established at the same time. If a second one is established, the first one goes down.
Workaround / action	Use only one tunnel for the same remote network, for example by extending the local network to include the former tunnels' local network.

Issue “Administrative Access From Moved Client in Single Stealth”

	Description
Synopsis	In single stealth auto detect and static modes the client cannot access the mGuard if the client was moved to the extern (unprotected) side.
Symptom	In single stealth mode the mGuard records the client computer's IP and MAC address at the internal (protected) interface and uses it to direct traffic to the client. If the client computer is moved to the extern (unprotected) side and tries to communicate with the mGuard (even using the management IP address) communication is not possible, as the mGuard still tries to direct the traffic to the internal (protected) side.
Workaround / action	Do connect another client computer to the internal (protected) interface so that mGuard can learn new addresses for IP and MAC or reboot the mGuard.

Issue “Config pull feedback incompatible with IDM 1.1.0 and 1.1.1”

	Description
Synopsis	Starting with firmware 5.0.0 the format of the HTTP queries used by the config pull procedure has changed. The new format cannot be understood by any Innominate Device Manager (IDM) version prior to 1.1.2.
Symptom	If devices operating firmware 5.0.0 are managed with an IDM prior to version 1.1.2, those devices's update status is not displayed correctly within IDM's device overview table. The update status does not change at all.
Workaround / action	Please update your IDM to version 1.1.2 or later.

Issue “Reconfiguration of the firewall does not block existing connections.”

	Description
Synopsis	Reconfiguration of firewall rules and similar changes do not affect established connections. The mGuard uses connection tracking tables to efficiently handle packets associated with connections which have already been accepted by the firewall. Upon reconfiguration of the firewall the connection tracking table is not flushed. Thus once allowed packets associated with established connections may still pass, though the current firewall rules block the establishment of like connections. Once a connection is terminated its related entry is removed from the connection tracking table and further traffic is blocked.
Symptom	Traffic associated with established connections may still pass, though the firewall was reconfigured to block it. New connection attempts are blocked as configured.
Workaround / action	Restart the mGuard after changing firewall rules and other configuration items which have to block traffic.

Issue “Particular self signed certificates not accepted as HTTPS client certificates”

	Description
Synopsis	Self signed certificates can be configured as acceptable certificates “per definition” if they are used by browsers to authenticate administrative access to the mGuard's GUI. Nonetheless such certificates are rejected if the command “`openssl verify -CAfile cert.crt -purpose sslclient cert.crt`” would verify them as invalid.
Symptom	Access is rejected by the mGuard, although the configured self-signed certificate is used by the browser.
Workaround / action	Create a different certificate having an appropriate or no key usage extension. For hints about which key usage extensions are missing, please check the output of the command “`openssl verify -issuer_checks -CAfile cert.crt -purpose sslclient cert.crt`“

Issue “Changed Flood Protection Settings delayed for VPN connections”

	Description
Synopsis	When settings are changed within the menu “Network Security / DOS Protection”, these do not become effective for VPN connections immediately, while they do for the incoming and outgoing firewall. The changed settings become effective as soon as VPN connections are restarted.
Symptom	Changed flood protection settings have no effect for established VPN connections.
Workaround / action	Restart the VPN connections or reboot the device.

Issue “Reconfiguration of VLAN ID not noticed by DHCP server”

	Description
Synopsis	If an mGuard is operated in *stealth mode* with a *DHCP* server on the *internal interface*, a reconfiguration of the VLAN ID is not noticed by the DHCP server. The DHCP server continues to use the old VLAN ID.
Symptom	After reconfiguration of the VLAN ID the internal DHCP server does no longer respond to requests from clients.
Workaround / action	Please disable and re-enable the DHCP server or restart the mGuard after such a configuration change.

Issue “Identical VPN connections just with different machine cert do no work”

	Description
Synopsis	If several VPN connections (at least two) are configured to use the same settings except for the local machine certificate and if they use a CA-certificate to authenticate remote sites the mGuard might assign incoming connections the wrong way.
Symptom	All incoming VPN connections are always assigned to the first VPN connection which matches the credentials provided by the peer. Thus the mGuard always uses the first machine certificate to authenticate itself to the remote side – even if the remote side is configured to accept the other machine certificate only. The connection attempt fails.
Workaround / action	Please distinguish your remote sites by issuing certificates from a different (sub-)certification authority for them. A different (sub-)CA-certificate is required per VPN connection. Sites to connect to the same connection must use certificates issued by the same CA-Certificate.

Issue “Transport mode VPN with %any as gateway not supported in stealth mode”

	Description
Synopsis	For any stealth mode operation the mGuard does not support the a VPN connection in transport mode with %any as gateway and CA authentication of several peers at once. Such scenarios do work only if just one peer connects.
Symptom	If more than one peer establishes a connection to the same transport mode VPN connection of the mGuard operating in stealth mode then packets might not get through the channel.
Workaround / action	Please use tunnel mode VPN connections.

Issue “Remote access ports not configurable for stealth(multi) with VLAN”

	Description
Synopsis	If an mGuard is operated in network mode “stealth” with “multiple clients” and has a VLAN ID configured for its management IP then HTTPS/SSH/SNMP remote access to that IP does only work if default ports are configured (443/22/161).
Symptom	If other than the default remote access ports are configured, no connection can be established to the management IP on those ports. The mGuard does not respond.
Workaround / action	Do not change the default ports.

Issue “Remote access ports not configurable for access via VPN”

	Description
Synopsis	If an mGuard is to be administrated through a VPN channel then HTTPS/SSH/SNMP remote access to the mGuard does only work if default ports are configured (443/22/161).
Symptom	If other than the default remote access ports are configured, no connection can be established to the mGuard through the VPN connection on those ports. The mGuard does not respond.
Workaround / action	Do not change the default ports.

Issue “Configuration Pull interferes with Firmware Update”

	Description
Synopsis	If a firmware update was started interactively and is performed on an mGuard which is retrieving a new configuration profile from an HTTPS server at the same time, then the configuration pull procedure may be disturbed by the firmware update and / or the firmware update may fail.
Symptom	The application of the new configuration profile may fail. If the “rollback” feature of the configuration pull procedure is used the mGuard may be rolled back to a configuration which is not equivalent to the one which was active before the start of the procedure or the mGuard may even “forget” to roll back to the former configuration though it was not possible to reach the HTTPS server any more after the new profile had been applied. The mGuard may fail to provide appropriate feedback to the IDM about the success or failure of the configuration pull procedure. The firmware update may fail. In particular this is likely to happen if the application of the profile initiates a reboot while the firmware update is still running.
Workaround / action	Either initiate the firmware update with the help of the configuration pull procedure or deactivate the configuration pull procedure for the time of the firmware update.

Issue “netadmin cannot perform a test download for the Configuration Pull” (bug #7868)

	Description
Synopsis	Through the GUI, the user “netadmin” cannot perform a test download of the configuration profile stored on a central HTTPS server.
Symptom	Even if the configuration is correct, “netadmin” will always see that the test download fails, for example with the message “The requested URL returned error: 401”.
Workaround / action	None

Issue “VPN tunnels with remote 1:1 NAT forward traffic for true network”

	Description
Synopsis	If a VPN tunnel is configured with remote 1:1 NAT enabled, then traffic destined for the true remote network as well as traffic destined for the virtual NATted remote network is forwarded through the tunnel if the source address also matches the tunnel's local network.
Symptom	Network traffic destined for the true remote network of a VPN tunnel is forwarded through the VPN tunnel also.
Workaround / action	Please (continue to) use one of the supported firmware versions before 7.0.0 if separated handling of these networks is a requirement.

Issue “Features not supported with firmware version 7.2.1”

	Description
Synopsis	Particular features are not supported with firmware version 1: •The Firewall Redundancy cannot be enabled. •For network mode “Stealth” the option “Listening for incoming VPN connections which are encapsulated” does not have the desired effect if enabled.
Symptom	The feature does not work, although its configuration is accepted by the mGuard.
Workaround / action	Please (continue to) use one of the supported firmware versions before 7.0.0.

4 Known Restrictions

- The Safari browser needs to have all sub-CA certificates installed in its trust store if they are used to authenticate for administrative access to the mGuard via X.509 certificate.
- The same browser instance cannot be used to administrate the mGuard with X.509 authentication and to login into the mGuard's user firewall at the same time.
- Configuration of the mGuard via its GUI (web access), via its Command Line Interface (shell access), and via SNMP must not happen concurrently. Concurrent configuration operations via different access methods may cause unexpected results.
- The external DHCP server of the mGuard cannot be used in multi stealth mode if a VLAN ID is assigned to the management IP.

5 Documentation Updates / Errata

- currently none